Triumph Learning Trust

Aspiration - Collaboration - Innovation

Data Protection Policy

Policy Details

Policy Level	Trust
Document Approver	Trust Board
Document Status	Final
Applicable to	All Trust Employees
Review Frequency	Every Year

Revision History

Revision	Date	Details	Approved by
0	28 April 2025	First Issue	PIC

Contents

1. Introduction

The trust aims to ensure that all personal data collected about staff, pupils, parents, trustees, governors, visitors and other individuals is collected, stored and processed in accordance with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018).

This policy applies to all personal data, regardless of whether it is in paper or electronic format. This policy applies to all staff employed by the trust, governors/trustees and to external organisations, volunteers and any other individuals working on the trusts behalf.

This policy does not form part of any individual's terms and conditions of employment with the trust and is not intended to have contractual effect. It does set out the trust's current practises and required standards of conduct. All are required to familiarise themselves with its content and comply with the provisions contained in it.

Breach of this policy will be treated as a disciplinary offence which may result in disciplinary action under the trust's Disciplinary Policy and Procedure up to and including summary dismissal depending on the seriousness of the breach.

Changes to data protection legislation will be monitored and further amendments to this policy may be required in order to remain compliant with legal obligations. Staff will be notified of any changes no later than one month from the date those changes are intended to take effect.

2. Scope of Policy

This policy meets the requirements of the UK GDPR and the provisions of the DPA 2018. It is based on guidance published by the Information Commissioner's Office (ICO) on the UK GDPR and the ICO's code of practice for subject access requests.

It meets the requirements of the Protection of Freedoms Act 2012 when referring to the trust's use of biometric data.

It also reflects the ICO's code of practice for the use of surveillance cameras and personal information.

In addition, this policy complies with the trust's funding agreement and articles of association.

3. Responsibilities

The Trust recognises it has a statutory obligation to adopt formal policies and establish workplace procedures for dealing with Data Protection. The Trust recognises that data protection rules and procedures promote good employment relations and is committed to dealing with matters in a fair and consistent way.

The Data Protection Officer

The data protection officer (DPO) is responsible for providing advice and guidance to the trust in order to assist the trust to implement this policy, monitor compliance with data protection

law, and develop related policies and guidelines where applicable. The DPO will carry out an annual audit of the trust's data processing activities and report to the trust their advice and recommendations on school data protection issues.

The DPO is also the first point of contact for individuals whose data the school processes, and for the ICO. The trust's DPO is the Warwickshire Legal Services School DPO Service and is contactable via schooldpo@warwickshire.gov.uk or alternatively

School Data Protection Officer, Warwickshire Legal Services, Warwickshire County Council, Shire Hall Market Square Warwick CV34 4RL

Data Protection Champions

The trust has nominated the following individuals as designated persons to be contacted internally in relation to all matters relating to data protection issues, and to make referrals, where necessary, to the Data Protection Officer:

Trust	Trust Estates and Compliance Advisor
Rugby Free Primary School	Operations Manager
Rugby Free Secondary School	Operations Manager
Alderman's Green Primary School	Operations Manager
Courthouse Green Primary School	Operations Manager

Please contact one of the 3 Data Protection Champions within the trust with any questions about the operation of this Data Protection Policy or the UK GDPR or if there are any concerns that this policy is not being or has not been followed.

Board of Trustees, as a corporate body, has the responsibility to set the strategic direction and objectives of all matters across the Trust.

The CEO takes overall responsibility for the implementation of policies and procedures, reports as appropriate to Trustees in relation to this Policy

Headteachers act as the representatives of the data controller on a day to day basis, implementation of and compliance within this policy within their schools.

All staff have a responsibility to:

- Comply with this policy and to co-operate with the schools' leadership and management on all matters relating to it
- Undertake any training recommended by their line manager
- Collect, store and process any personal data in accordance with this policy
- Inform the school of any changes to their personal data, such as a change of address
- Contact the designated Data Protection Champions in the following circumstances:
    - With any questions about the operation of this policy, data protection law, retaining personal data or keeping personal data secure
    - If they have any concerns that this policy is not being followed
    - If they are unsure whether or not they have a lawful basis to use personal data

in a particular way

- If they need to rely on or capture consent, draft a privacy notice, deal with data protection rights invoked by an individual, or transfer personal data outside the European Economic Area
- If there has been a data breach
- Whenever they are engaging in a new activity that may affect the privacy rights of individuals
- If they need help with any contracts or sharing personal data with third parties

Employees may have access to the personal data of other members of staff, suppliers, parents or pupils of the trust in the course of their employment or engagement. If so, the trusts expect those employees to help meet the organisations data protection obligations to those individuals. Specifically, all staff members must:

- Only access the personal data including photographs that they have authority to access, and only for authorised purposes
- Only allow others to access personal data if they have appropriate authorisation
- Keep personal data secure (for example by complying with rules on access to trust premises, computer access, password protection and secure file storage and destruction)
- Not to remove personal data including photographs or devices (including mobile phones) containing personal data from the trust premises unless appropriate security measures are in place (such as pseudonymisation, encryption, password protection) to secure the information
- Not to store personal information on local drives, personal mobile devices and mobile phones.

4. The Data Controller

Triumph Learning Trust processes personal data relating to parents, pupils, staff, governors, volunteers, visitors and others, and therefore is a data controller.
The trust is registered as a data controller with the ICO and will renew this registration annually or as otherwise legally required.

5. When can the Trust or School Process Personal Data?

Data Protection Principles

The UK GDPR is based on data protection principles relating to the processing of personal data that the trust must comply with. The trust has adopted the principles to underpin this UK GDPR and Data Protection Policy.
The principles require that all personal data shall be:

- Processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency')

- Used and collected only for specified, explicit and legitimate purposes ('purpose limitation')
- Used in a way that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation')
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy')
- Not be kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the data is processed ('storage limitation')
- Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage ('integrity and confidentiality').
- This policy sets out how Trust aims to comply with these principles.

Lawfulness, Fairness and Transparency

The trust only collects, process and share personal data fairly and lawfully and for specified purposes. It must have a specified purpose for processing personal data and special category of data as set out in the UK GDPR.

Before the processing starts for the first time the trust (and the schools) will review the purposes of the particular processing activity and select the most appropriate lawful basis for that processing. The trust will then regularly review those purposes whilst processing continues in order to confirm that the processing is necessary for the purpose of the relevant lawful basis (i.e. that there is no other reasonable way to achieve that purpose).

Personal Data

The trust may only process a data subject's personal data if one of the following legal reasons are available:

- The data subject has given their consent
- The processing is necessary for the performance of a contract with the data subject or for taking steps at their request to enter into a contract
- To protect the data subject's vital interests
- To meet their legal compliance obligations (other than a contractual obligation)
- To perform a task in the public interest or in order to carry out official functions as authorised by law; or
- For the purposes of the trust's legitimate interests were authorised in accordance with data protection legislation. This is provided that processing is necessary for the purposes of the legitimate interests pursued by the trust or by a third party except where such interests are overridden by the interests or rights and freedoms of the individual.

Special Category Data

The trust may only process special category data if they are entitled to process personal data (using one of the legal reasons above) and one of the following conditions are met:

- The data subject has given their explicit consent
- The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed on the trust in the field of employment law, social security, law or social protection law. This may include, but is not limited to, dealing with sickness, absence, dealing with a disability and adjusting for the same, arranging private health care insurance and providing contractual sick pay
- To protect the data subject's vital interests
- Processing carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
- To meet their legal compliance obligations (other than a contractual obligation)
- Where the data has been made public by the data subject
- To perform a task necessary for reasons of substantial public interest
- Where it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services
- Where it is necessary for reasons of public interest in the area of public health
- The processing is necessary for archiving, statistical or research purposes
- The process is necessary for establishing, exercising or defending legal claims
- The trust and its schools must identify and document the legal grounds being relied upon for each processing activity

Consent

Where the trust relies on consent as a legal reason for processing (as set out above), it will adhere to the requirements set out in the UK GDPR.

Consent must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they signify agreement to the processing of personal data relating to them. Explicit consent requires a very clear and specific statement to be relied upon (i.e. more than just mere action is required).

A data subject will have consented to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity will not amount to valid consent.

Data subjects must be easily able to withdraw consent to processing at any time and withdrawal must be promptly honoured.

If explicit consent is required, the trust will normally seek another legal basis to process that data. However, if explicit consent is not required the trust will normally seek another legal basis.

The trust will keep records of consents obtained in order to demonstrate compliance with consent requirements under the UK GDPR.

If the trust offers online services to pupils, such as classroom apps, and intend to rely on consent as a basis for processing, the specific school will get parental consent where the pupil is under 13 (except for online counselling and preventive services).

Purpose Limitation

The trust will only collect personal data for specified explicit and legitimate reasons. The trust will explain these reasons to the individuals when their personal data is first collected.
If the trust wants to use personal data for reasons other than those given when they first obtained it, they will inform the individuals concerned before they do so and seek consent where necessary.

Data Minimisation

The trust will only process personal data when statutory obligations and duties require them to do so. When personal data is no longer needed for specified purposes, the trust will delete or anonymise the data in line with the Records Management and Retention Policy

Accuracy

The trust will endeavour to correct or delete any inaccurate data being processed by checking the accuracy of the personal data at the point of collection and at regular intervals afterwards. Data subjects also have an obligation to ensure that their data is accurate, complete, up to date and relevant. Data subjects have the right to request rectification to incomplete or inaccurate data held by the trust. Please see section 10 (Data Subjects Rights and Requests).

Storage Limitation

Legitimate purposes for which the data is processed may include satisfying legal, accounting or reporting requirements. The trust will ensure that they adhere to legal timeframes for retaining data. The trust will take reasonable steps to destroy or erase from their systems all personal data that they no longer require. They will also ensure that the data subjects are informed of the period for which data is stored and how that period is determined in their privacy notices. Please refer to the Records Management and Retention Policy for further details about how the trust retains and removes data.

Integrity and Confidentiality

The trust will protect personal data and keep it safe from unauthorised or unlawful access, alteration, processing or disclosure, and against accidental or unlawful loss, destruction or damage. In particular:

- Paper-based records and portable electronic devices, such as laptops and hard drives that contain personal data are kept under lock and key when not in use
- Papers containing confidential personal data must not be left on office and classroom

desks, on staffroom tables, pinned to notice/display boards, or left anywhere else where there is general access

- Staff must ensure passwords are hard for anyone else to guess by incorporating numbers and mixed case into it
- Encryption software is used to protect all portable devices and removable media on which personal information is stored, such as laptops and USB devices
- Staff, pupils or governors who store personal information on their personal devices are expected to follow the same security procedures as for school-owned equipment
- Where the trust needs to share personal data with a third party, they will carry out due diligence and take reasonable steps to ensure it is stored securely and adequately protected (see section 4)
- Pseudonymisation (this is where the trust replaces information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person to whom the data relates cannot be identified without the use of additional information which is meant to be kept separately and secure)
- Ensuring authorised access (i.e. that only people who have a need to know personal data are authorised to access it).

6. Sharing Personal Data

The trust will not normally share personal data with third parties as set out in the Privacy Notices, unless certain safeguards and contractual arrangements have been put in place. The UK GDPR and the DPA 2018 also allow information to be shared where:

- There is an issue with a pupil or parent/carer that puts the safety of their staff at risk
- They need to liaise with other agencies – they will seek consent as necessary before doing this
- Their suppliers or contractors need data to enable them to provide services to staff and pupils – for example, IT companies. When doing this, the trust will:
    - Only appoint suppliers or contractors which can provide sufficient guarantees that they comply with data protection law
    - Establish a data sharing agreement with the supplier or contractor, either in the contract or as a standalone agreement, to ensure the fair and lawful processing of any personal data the trust share
    - Only share data that the supplier or contractor needs to carry out their service, and information necessary to keep them safe while working with us

The trust will also share personal data with law enforcement and government bodies (e.g. the Local Authority, Ofsted and the Department of Health) where they are legally required to do

so or in the best interests of their pupils, parents or staff. They will share this data for the following reasons:

- The prevention or detection of crime and/or fraud
- The apprehension or prosecution of offenders
- The assessment or collection of tax owed to HMRC
- In connection with legal proceedings
- Where the disclosure is required to satisfy their safeguarding obligations
- Research and statistical purposes, as long as personal data is sufficiently anonymised, or consent has been provided

These authorities are up to date with data protection law and have their own policies relating to the protection of any data that they receive or collect. The intention to share data relating to individuals to an organisation outside of the trust shall be clearly defined within written notifications and details and basis for sharing that data given. The trust may also share personal data with emergency services and local authorities to help them to respond to an emergency situation that affects any of their pupils or staff.

Transfer of Data outside the European Economic Area (EEA)

The trust will not transfer data to another country outside of the EEA without appropriate safeguards being in place and in compliance with the UK GDPR. All staff must comply with the trust's guidelines on transferring data outside of the EEA. For the avoidance of doubt, a transfer of data to another country can occur when data is transmitted, sent, viewed or accessed in that particular country.

Storing your personal information outside the UK

When personal information is stored outside the UK, we will make sure we keep it safe.

Most personal information we collect, and use is stored on systems in the UK and EEA.

On occasion, your information may leave the UK or EEA:

- To get to another organisation
- If it is stored in a system outside the EEA

Details of these transfers can be found in the Privacy Notices

When this happens, we make sure the country it is sent to has the required level of data protection. We also take additional steps to protect your information including:

- Making sure it is transferred securely
- There is a contract in place which ensures the recipient will protect your information

Where we have to send personal information to a country without an adequacy decision, we carry out due diligence to ensure that the transfer is made in accordance with UK data protection legislation.

7. Data Subject Rights and Requests

Subject Access requests

A Data Subject has the right to make a 'subject access request' to gain access to the personal information that the trust holds on them. This includes:

- Confirmation that their data is being processed
- Access to their a copy of the personal data
- A description of the information that is being processed
- The purpose for which the information is being processed
- The categories of personal data concerned
- The recipients/class of recipients to whom that information is or may be disclosed
- Details of the trust's sources of information obtained
- How long the data will be stored for, or if this isn't possible, the criteria used to determine this period
- Any Personal Data processed for the purposes of evaluating matters in relation to the Data Subject that has constituted or is likely to constitute the sole basis for any decision significantly affecting him or her, to be informed of the logic of the Data Controller's decision making. Such data may include, but is not limited to, performance at work, creditworthiness, reliability and conduct
- Other supplementary information.

How to make a subject access request Any data subject who wishes to obtain the above information may make the request in writing or verbally. To enable the request to be accurately responded to, the applicant should make the request in writing and set out:

- Name of individual
- Name of the school
- Correspondence address
- Contact number and email address
- Details of the information requested

The request should in the first instance be sent to tlt-sar@triumphlearning.org

If staff receive a subject access request, they must immediately forward it to a Data Protection Champion who will inform the DPO.

Children and Subject Access Requests

Personal data about a child belongs to that child, and not the child's parents or carers. For a parent or carer to make a subject access request with respect to their child, the person should have parental responsibility for the child, and the child must either be unable to understand their rights and the implications of a subject access request or have given their consent.

Children aged 13 and above are generally regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at their school aged 13 and above may not be granted without the express permission of the pupil.

Children below the age of 13 are generally not regarded to be mature enough to understand their rights and the implications of a subject access request. Therefore, subject access requests from those with parental responsibility for pupils at their school [aged under 13] will in general be granted without requiring the express permission of the pupil. These are not fixed rules and a pupil's ability to understand their rights will always be judged on a case-by-case basis.

Responding to a Subject Access Request

When responding to requests, the trust:

- May ask the individual to provide 2 forms of identification
- May contact the individual via phone to confirm the request was made
- Will respond without delay and within 1 month of receipt of the request
- Will provide the information free of charge
- May tell the individual the trust will comply within 3 months of receipt of the request, where a request is complex or numerous, or where it is impractical to comply within a month due to school closure. The trust will inform the individual of this within 1 month, and explain why the extension is necessary

The trust will not disclose information if it:

- Might cause serious harm to the physical or mental health of the pupil or another individual
- Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
- Is contained in adoption or parental order records
- Would include another person's personal data that we can't reasonably anonymise, and we don't have the other person's consent and it would be unreasonable to proceed without it
- Is part of certain sensitive documents, such as those related to crime, immigration, legal proceedings or legal professional privilege, management forecasts, negotiations, confidential references, or exam scripts
- Is given to a court in proceedings concerning the child

If the request is unfounded or excessive, the trust may refuse to act on it or charge a reasonable fee which considers administrative costs. A request will be deemed to be unfounded or excessive if it is repetitive or asks for further copies of the same information.

When the trust refuses a request, it will tell the individual why and tell them they have the right to complain to the ICO.

Other Data Protection Rights of the individual

In addition to the right to make a subject access request (see above), and to receive information in relation to how the trust collect personal data and how they use/process it, individuals also have the right to:

- (Where consent is relied upon as a condition of processing) to withdraw consent to processing at any time where processing is based on consent of the pupil or parent
- Receive certain information about the trust's processing activities
- Ask us to rectify (inaccurate or incomplete data), erase (if it is no longer in relation to the purposes for which it was collected or processed) or restrict processing of their personal data
- Prevent use of their personal data for direct marketing
- Challenge processing which has been justified on the basis of their legitimate interests or in the public interest
- Request a copy of an agreement under which personal data is transferred outside of the European Economic Area
- Object to decisions based solely on automated decision making or profiling (decisions taken with no human involvement, that might negatively affect them)
- Prevent processing that is likely to cause damage or distress to the data subject or anyone else
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms
- Make a complaint to the ICO
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Individuals should submit any request to exercise these rights to the DPO. If staff receive such a request, they must immediately forward it to the Data Protection Champion who will send it to the DPO for information purposes. If any request is made to exercise the rights above, it is a requirement for the Data Protection Champion to verify the identity of the individual making the request.

8. Biometric Recognition Systems

Where the trust uses pupils' and staff biometric data as part of an automated biometric recognition system (for example, use fingerprints to receive school dinners instead of paying with cash at Rugby Free Secondary School), the trust will comply with the requirements of the Protection of Freedoms Act 2012.

Parents / carers will be notified before any biometric recognition system is put in place or before their child first takes part in it.

The trust will get written consent from at least one parent or carer or the staff member themselves before any biometric data is taken and processed. Parents/carers and pupils have the right to choose not to use the trust's biometric systems. In such cases, trust will provide an alternative means of accessing the relevant services for those individuals. For example, students can use a pin or a 'ParentPay Card' instead of their fingerprints. Parents/carers and pupils can object to participation in the school's biometric recognition system(s), or withdraw consent, at any time, and the trust will make sure that any relevant data already captured is deleted. If a student under the age of 18 objects to the processing of their Biometric data, this will override the consent of the parents/carers and processing will not continue under any circumstances.

Where staff members or other adults use the school's biometric system(s), the trust will also obtain their consent before they first take part in it and provide alternative means of accessing the relevant service if they object. Staff and other adults can also withdraw consent at any time, and the school will delete any relevant data already captured.

The Protection of Freedoms Act 2012 only covers processing on behalf of the trust. If a pupil is using biometric software for their own personal purposes (e.g. facial recognition technology) this is classed as private use not processing by the trust, even if the software is accessed using school or college equipment.

9. CCTV

The trusts use CCTV in various locations around the school site to ensure it remains safe. The trust will adhere to the ICO's code of practice for the use of CCTV. The trust does not need to ask individuals' permission to use CCTV, but the trust make it clear where individuals are being recorded. Security cameras are clearly visible and accompanied by prominent signs explaining that CCTV is in use. Any enquiries about the CCTV system should be directed to:

Trust	Trust Estates and Compliance Advisor
Rugby Free Primary School	Operations Manager
Rugby Free Secondary School	Operations Manager
Alderman's Green Primary School	Operations Manager

10.Photograph and Videos

As part of the trust's activities, the schools may take photographs and record images of individuals within the school. The trust will obtain written consent from parents/carers for photographs and videos to be taken of their child for communication, marketing and promotional materials. The trust will clearly explain how the photograph and/or video will be used to both the parent/carer and pupil. Uses may include:

- Within school on notice boards and in school magazines, brochures, newsletters, etc
- Outside of school by external agencies such as the school photographer, newspapers, campaigns
- Online on the trust websites or social media pages

Consent can be refused or withdrawn at any time. If consent is withdrawn, the trust will delete the photograph or video and not distribute it further. When using photographs and videos in this way the trust will not accompany them with any other personal information about the child, to ensure they cannot be identified. See the specific school child protection and safeguarding policy for more information on their use of photographs and video

11. Data Protection by Design and Default

The trust will put measures in place to show that it has integrated data protection into all of its data processing activities, including:

- Appointing a suitably qualified DPO, and ensuring they have the necessary resources to fulfil their duties and maintain their expert knowledge
- Only processing personal data that is necessary for each specific purpose of processing, and always in line with the data protection principles set out in relevant data protection law (see section 3)
- Completing privacy impact assessments where the school's processing of personal data presents a high risk to rights and freedoms of individuals, and when introducing new technologies (the DPO will advise on this process)
- Integrating data protection into internal documents including this policy, any related policies and privacy notices
- Training members of staff on data protection law, this policy, any related policies and any other data protection matters; the trust will also keep a record of attendance
- Regularly conducting reviews and audits to test their privacy measures and make sure the trust is compliant
- Maintaining records of their processing activities, including:
    - For the benefit of data subjects, making available the name and contact details of their school and DPO and all information the trust are required to share about how the organisation use and process their personal data (via their privacy notices)
    - For all personal data that the trust holds, maintaining an internal record of the type of data, data subject, how and why the trust is using the data, any third-party recipients, how and why the trust are storing the data, retention periods and how the organisation is keeping the data secure.

Data Protection Impact Assessment (DPIA's)

The trust will conduct DPIAs for any new technologies or programmes being used by the trust which could affect the processing of personal data. In any event the trust carries out DPIAs when required by the UK GDPR in the following circumstances:

- For the use of new technologies (programs, systems or processes) or changing technologies
- For the use of automated processing

- For large scale processing of special category data
- For large scale, systematic monitoring of a publicly accessible area (through the use of CCTV)

Our DPIAs contain:

- A description of the processing, its purposes and any legitimate interests used
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance.

12.Disposal of Records

Personal data that is no longer needed will be disposed of securely. Personal data that has become inaccurate or out of date will also be disposed of securely, where the trust cannot or do not need to rectify or update it.

For example, the trust will shred or incinerate paper-based records and overwrite or delete electronic files. The trust may also use a third party to safely dispose of records on their behalf. If the trust does so, they will require the third party to provide sufficient guarantees that it complies with data protection law. Please see the Records Management and Retention Policy.

13.Personal Data Breaches

The trust shall take all reasonable steps to ensure that there are no personal data breaches. In the unlikely event of a suspected data breach, the trust will follow the procedure set out in Appendix 2. When appropriate, the trust shall report the data breach to the ICO within 72 hours. Such breaches in a trust context may include, but are not limited to:

- A non-anonymised dataset being published on the school's website which shows the exam results of pupils eligible for the pupil premium
- Safeguarding information being made available to an unauthorised person
- The theft of a school laptop containing non-encrypted personal data about pupils

14.Training

The trust will ensure all relevant personnel have undergone adequate training to enable them to comply with data privacy laws. New staff are provided with data protection training as part of their induction process. Data protection will also form part of continuing professional development, where changes to legislation, guidance or the school's processes make it necessary.

15.Audit

The trust regularly tests its data systems and processes through the DPO in order to assess compliance. These are done through data audits which take place annually in order to review use of personal data.

16.Appendices

Appendix 1	The Role of the DPO
Appendix 2	Personal Data Breach Procedure
Appendix 3	Subject Access Request Procedure
Appendix 4	Definitions

Appendix 1 – The Role of the DPO

The DPO should be contacted in the following circumstances if the trust:

- Is unsure of the lawful basis being relied on to process personal data
- Needs to rely on consent as a fair reason for processing (please see section 3 for further detail)
- Needs to draft privacy notices or fair processing notices
- Are unsure about the retention periods for the personal data being processed
- Is unsure about what security measures need to be put in place to protect personal data
- Has had a personal data breach
- Is unsure on what basis to transfer personal data outside the EEA
- Needs any assistance dealing with any rights invoked by a data subject
- Is engaging in a significant new (or a change in) processing activity which is likely to require a data protection impact assessment or if they plan to use personal data for purposes other than what it was collected for
- Plans to undertake any activities involving automated processing or automated decision making
- Needs help complying with applicable law when carrying out direct marketing activities
- Needs help with any contracts or other areas in relation to sharing personal data with third parties

Appendix 2 – Personal Data Breach Procedure

Introduction

This procedure defines personal data breaches and sets out the steps staff need to follow in the case of a suspected breach. If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it in accordance with this procedure.

This procedure is based on guidance on personal data breaches produced by the Information Commissioner's Office (ICO).

What is personal data breach?

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This means that a breach is more than just losing personal data.

Examples of how a breach may occur include:

- Theft of data or equipment on which data is stored, such as a laptop containing non-encrypted sensitive personal data or the school cashless catering payment provider being hacked and parents' financial details stolen
- Loss of data or equipment on which data is stored
- Inappropriate access controls allowing unauthorised use
- Accidental Loss
- Destruction of personal data
- Damage to personal data
- Equipment failure
- Unlawful disclosure of personal data to a third party
- Human error such as hard copies of reports being sent to the wrong family
- Unforeseen circumstances such as fire or flood
- Hacking attack
- 'Blagging' offences or social engineering where information is obtained by deceiving the organisation which holds it

Personal data breach procedure

1. On the occurrence or discovery of a breach, or potential breach, the staff member or data processor must immediately notify the Data Protection Champion.

   The Data Protection Champion will assess whether a breach of personal information has occurred, the level of severity (Please see *Assessing the Risks* below) and act to contain the breach as soon as is reasonably practical and also inform the Headteacher/CEO and GDPR Champion. They should complete the Data Security Incident Report providing details including the reporter's name, the date/time of the breach, the date/time of detecting the breach, and basic information about the type

of breach and personal data concerned and any mitigating actions that have been taken to contain the breach.

The Data Protection Champion will assess the level of risk posed by the breach and if the risk of harm to any individual is low (e.g. because no personal information has left the control of the school), then the Data Protection Champion will undertake an internal investigation to consider whether the information security policy was followed, and whether any alterations need to be made to internal procedures as a result. The breach will be recorded as a 'near-miss'.

Staff will cooperate with the investigation (including allowing access to information and responding to questions). The investigation will not be treated as a disciplinary investigation.

2. In all other cases, the Data Protection Champion/GDPR Lead will notify the Data Protection Officer GDPR. The DPO will assess the potential consequences, based on how serious they are, and how likely they are to happen and advise staff on the appropriate containment steps to or contain the breach to mitigate / minimize the risks to those individuals affected by it. The Data Protection Champion and GDPR lead will make all reasonable efforts to contain and minimise the impact of the breach, assisted by relevant staff members or data processors where necessary.
3. The DPO will work with the GDPR lead to ascertain as to whether the breach must be reported to the ICO. This must be judged on a case-by-case basis. To decide, the DPO will consider whether the breach is likely to negatively affect people's rights and freedoms, and cause them any physical, material or non-material damage (e.g. emotional distress), including through:
    - Loss of control over their data
    - Discrimination
    - Identify theft or fraud
    - Financial loss
    - Unauthorised reversal of pseudonymisation (for example, key-coding)
    - Damage to reputation
    - Loss of confidentiality
    - Any other significant economic or social disadvantage to the individual(s) concerned If it is likely that there will be a risk to people's rights and freedoms, the trust must notify the ICO.

    The DPO may use the ICO's self-assessment tool to determine whether to report the breach to the ICO.
4. Where the DPO recommend that the breach be reported to the ICO, the trust as the data controller will report the initial breach to the ICO wither via the 'report a breach' page on the ICO website or through the breach report line (0303 123 1113), within 72 hours of the trust's becoming aware of the breach.

The trust will set out:

- A description of the nature of the personal data breach including, where possible:
    - The categories and approximate number of individuals concerned
    - The categories and approximate number of personal data records concerned
- The name and contact details of the DPO
- A description of the likely consequences of the personal data breach
- A description of the measures that have been, or will be taken, to deal with the breach and mitigate any possible adverse effects on the individual(s) concerned

If all the details the details relating to the breach are not yet known, the trust will report as much as they can within 72 hours explaining the delay, the reasons why, and when the DPO expects to have further information. The trust will submit the remaining information as soon as possible.
The decision will be documented (either way), in case it is challenged at a later date by the ICO or an individual affected by the breach.

5. After the initial report, the DPO may liaise with the ICO on behalf of the trust.
6. The DPO and the GDPR Lead/Champion will also assess the risk to individuals, again based on the severity and likelihood of potential or actual impact. If the risk is high, the individuals whose data has been breached will all be informed in writing. The notification will set out:
    - The name and contact details of the DPO
    - A description of the likely consequences of the personal data breach
    - A description of the measures that have been, or will be, taken to deal with the data breach and mitigate any possible adverse effects on the individual(s) concerned
7. The GDPR Lead/Data Protection Champion's will notify any relevant third parties who can help mitigate the loss to individuals – for example, the police, insurers, banks or credit card companies.
8. The Data Protection Champion's and GDPR Lead will document each breach, irrespective of whether it is reported to the ICO in the Data Breach log. For each breach, the record will include the facts and cause, effects and action taken to contain it and ensure it does not happen again (such as establishing more robust processes or providing further training for individuals). Records of all breaches will be stored securely.
9. The Data Protection Champion/GDPR Lead and headteacher will meet to review the breach and recommend and implement any recommended improvements to ensure it does not happen again. This meeting will happen as soon as reasonably possible.

Assessing the risks

Levels of risk can be very different and vary on an individual breach of data security depending what is lost/damaged/stolen. The Data Protection Champion should consider the following:

- The type of data involved and its sensitivity
- Whether the data has been lost or stolen and whether there are any protections in place such as encryption
- What has happened to the data? If data has been stolen, could it be used for purposes which are harmful to the individuals to whom the data relate? If it has been damaged, this poses a different type and level of risk. Regardless of what has happened to the data, what could the data tell a third party about the individual? Sensitive data could mean very little to an opportunistic laptop thief while the loss of apparently trivial snippets of information could help a determined fraudster build up a detailed picture of other people
- The number of individuals (the data subjects) affected by the breach, who those individuals are and the harm that could come to them. Are there risks to physical safety or reputation, of financial loss or a combination of these and other aspects of their life? Are there wider consequences to consider such as a risk to life?
- A loss of public confidence in the trust as a result of the breach.

All staff, Governors and Trustees should establish whether there is anything they can do to recover any losses and limit the damage the breach can cause.

Containment and Recovery

The trust's initial response will be to investigate, contain the situation and implement recovery plan including, damage limitation. The trust may need input from specialists such as IT, HR and legal and in some cases contact with external third parties to Seek assistance in the containment exercise. Containment could include:

- Isolating or closing a compromised section of the network, recovery of released documents, finding a lost piece of equipment or simply changing any related access codes
- Establishing whether there is anything the trust can do to recover any losses and limit the damage the breach can cause
- The physical recovery of equipment could involve the use of backup records to restore lost or damaged data or ensuring that staff recognise when someone tries to use stolen data to access accounts
- Considering whether any individual affected by the data breach should be notified.

Actions to minimise the impact of data breaches

The trust will take the actions set out below to mitigate the impact of different types of data breach. For example, if sensitive information is disclosed via email (such as safeguarding records)

- If special category data (sensitive information) is accidentally made available via email to unauthorised individuals, the sender must attempt to recall the email as soon as they become aware of the error
- Members of staff who receive personal data sent in error must alert the sender and the Data Protection Champion as soon as they become aware of the error. The Data Protection Champion will alert the DPO as soon as they become aware
- If the sender is unavailable or cannot recall the email for any reason, the Data Protection Champion will ask the IT department to recall it
- In any cases where the recall is unsuccessful, the Data Protection Champion will contact the relevant unauthorised individuals who received the email, explain that the information was sent in error, and request that those individuals delete the information and do not share, publish, save or replicate it in any way
- The Data Protection Champion will ensure the trust receives a written response from all the individuals who received the data, confirming that they have complied with this request
- The Data Protection Champion will carry out an internet search to check that the information has not been made public; if it has, the trust will contact the publisher/website owner or administrator to request that the information is removed from the website and deleted
- If safeguarding information is compromised, the data protection champion/GDPR Lead will inform the designated safeguarding lead and discuss whether the school should inform any, or all, of its local safeguarding partners

Appendix 3 – Subject Access Request Procedure

This procedure applies to all personal data processed by the trust excluding personal data that is asked for as a matter of routine by data subjects. Any request is valid (not matter the legislation referenced) and any member of staff can receive one. It is therefore vital that all staff understand this procedure and are able to recognise a SAR

Data subjects are entitled to exercise their right of access under the UK General Data Protection Regulations (UK GDPR) to any personal data about themselves and, if the request is valid, be provided with the requested information in an easy to access format, free of charge, within one calendar month of the request.

This procedure is applicable for all staff (permanent, contracted, volunteer or otherwise).

All staff:

- Are responsible for ensuring that any request for information they receive is dealt with in line with the requirements of the UK GDPR by following this procedure
- Have a responsibility to recognise a request for information and ensure it is passed to the responsible Data Protection champion within two working days.

Any requests will be held on file for a 12-month period at which point it will be securely destroyed.

How to recognise a valid Subject Access Request (SAR)

SARs can be made verbally or in writing in, including by letter, fax or by electronic means for example: by e-mail, website form, texts, Facebook or Twitter. They include all requests for personal data, whether or not the data subject has referred to data protection or SAR and including requests which refer to FOI instead.

The SAR Procedure

The objective of the procedure is to ensure that the request is received and documented properly so that the nominated Data Protection Champion can respond to the request in a correct and timely manner.

General Staff role:

When a request is received from a Data Subject the staff member must inform the Data Protection Champion immediately or at least within 2 working days.
Data Protection Champion Role:

- Record the request in the log, qualify the request and confirm the identity of the individuals making the request. Witness two pieces of ID such as a birth certificate, passport, driving licence, official letter addressed to the requester at their home address e.g. recent bank statement, recent utilities bill or council tax bill. The documents should include the requesters name, date of birth and current address. Do not take copies of the ID.
- If they individual has requested information on behalf of a child, request proof that they have parental responsibility for the child. This may already be recorded on the Schools MIS system. If the child is 13 years or older, the data protection champion

should consult the DPO and relevant parties at each school to determine seeking the child's permission.These will be considered on a case by case basis.

- Evaluate the request with the Senior Leadership Team at the school and identify all records that need checking. If the request is excessive / repetitive, the data protection champion should contact the parent to try and narrow down their request. If the request is complex and requires further consideration contact the School DPO Service.
- Write to the requester outlining that the request has been received and the timeframe. The time available under UK GDPR is one calendar month to provide the information free of charge, unless a request is manifestly unfounded or excessive/repetitive. As the timeframe depends on the month in which the request is made, the champion should aim for a time span of 28 days. If the request is judged unfounded or excessive, formally respond to the request stating the judgement.
- Oversee the compilation of the information and discuss with the School Senior Leadership team and redact any records where the disclosure of personal information:
    - Might cause serious harm to the physical or mental health of the pupil or another individual
    - Would reveal that the child is at risk of abuse, where the disclosure of that information would not be in the child's best interests
    - Is contained in adoption or parental order records
    - Is given to a court in proceedings concerning the child
    - Mentions a third party or has a third party at its focus.

Documents should be redacted with either a specialised black redaction pen. The records should then be photocopied and the photocopy given to the requester.

- Compile the requested data and send to the school senior leadership team/GDPR Lead for a final check and sign off.
- If the request is particularly complex, it can be sent to the DPO for checks.
- Formally respond to the request. If the request was made electronically (digitally), the information should be provided in a commonly used electronic format. If the request has been refused outline the reasons why and explain that they have the right to complain to the ICO.
- Document the request in the log and keep a secure record of all paperwork and correspondence.

Further Consideration

What I must do?	Why?	How
Be clear about the nature of the request and identify what information is being requested.	Clarity about the nature of the request will enable you to decide whether the request needs to be dealt with in	Review the request and identify: If the request is for the personal information of the requester or made by an individual on behalf of

	accordance with statutory requirements, who needs to deal with the request, and/or whether this is business as usual (BAU). If necessary ask the individual for clarity	another person (e.g. on behalf of a child or an adult lacking capacity) – this is a subject access request; If the request is for nonpersonal information – this may be dealt with as BAU or formally under the Freedom of Information Act 2000 (the FOIA) or the Environmental Information Regulations 2004 (the EIR). **NB: The request can be received in a range of different formats e.g. letter, email, a completed form, or can be made via social media (e.g. a Facebook page or Twitter account)**
If the request is a SAR the request must be forwarded to the Data Protection Champion within two working days of receipt of the request.	The UK GDPR stipulates that SARs must be completed within one month of the request – but in reality, as soon as possible.	Forward the request to the Data Protection Champion.
If the information requested is for non-personal information i.e. is organisational or statistical information, this will fall under the FOIA or EIR, or BAU and will be dealt with, as follows: All non-routine FOIA or EIR requests must be forwarded to the responsible member of staff (usually the Headteacher) and the Data Protection Champion within two working days of receipt of the request	The FOIA and EIR stipulates that requests must be completed within 20 working days of the request – therefore the more swiftly requests are dealt with, the more likely the organisation will meet its statutory deadlines. BAU requests need to be dealt with by an individual in that particular service area who can identify and locate the information requested and provide a response within a reasonable timeframe.	If the request is for none routine/FOIA/EIR information, contact the data protection champion.
If the information requested is for the personal information of an individual for use in a criminal investigation by the police, or any other agency investigating criminal offences, this will fall under either the regulatory Investigative Powers Act 2000 (RIPA) or Data Protection.	It is in the public interest that requests are identified and dealt with as quickly as possible.	Scan and email the request to the Data Protection Champion who will contact the DPO immediately.

Appendix 4 – Definitions

Personal Data	Any information relating to an individual where the individual can be identified (directly or indirectly) from that data alone or in combination with other identifiers the trust possesses or can reasonably access. Personal data can include factual data (this includes: name, initials email address, location data or date of birth), identification number, an online identifier (such as username), opinions about that person's actions or behaviours and - special category data and pseudonymised personal data. It may also include factors specific to the individual's physical, physiological, genetic, mental, economic, cultural or social identity. Personal data will be stored either electronically or as part of a structured manual filing system in such a way that it can be retrieved automatically by reference to the individual or criteria relating to that individual. Anonymous data or data that has had the identity of an individual permanently removed is not classed as personal data. Information about companies or public authorities is not personal data
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes
Special Data	Previously termed 'Sensitive Personal Data', is more sensitive personal data and so needs more protection, The UK GDPR defines special category data as: personal data revealing **racial or ethnic origin**; personal data revealing **political opinions**; personal data revealing **religious or philosophical beliefs**; personal data revealing **trade union membership**; **genetic data**; **biometric data** (where used for identification purposes); data concerning **health**; data concerning a person's **sex life**; and data concerning a person's **sexual orientation**.
Biometric Data	Defined as personal data relating to the physical, physiological or behavioural characteristic of an individual which allows the identification of that individual. This can include their fingerprints, facial shape, retina and iris patterns, and hand measurements. An automated biometric recognition system uses technology which measures an individual's physical or behavioural characteristics by using equipment that operates 'automatically' (i.e. electronically). Information from the individual is automatically compared with biometric information stored in the system to see if there is a match in order to recognise or identify

	the individual. For example, where a fingerprint is used to identify an individual and allow them access to an account.
Data Subject	The identified or identifiable individual whose personal data is held or processed is known as the Data Subject. This includes but is not limited to staff, students, parents/carers and governors/trustees.
Data Controller	A person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Only controllers need to pay the data protection fee.
Data Processor	A person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	Any activity that involves the use of personal data. This includes but is not limited to collecting, recording, and storing data, carrying out any operation or set of operations on that data such as organising, adapting, amending, retrieving, using, structuring, disclosing, erasing or destroying it and transmitting or transferring personal data to third parties. The process can be automated or manual.
Automated Processing	Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. An example of automated processing includes profiling and automated decision making. Automatic decision-making is when a decision is made which is based solely on automated processing which produces legal effects or significantly affects an individual. Automated decision making is prohibited except in exceptional circumstances.
Data Protection Impact Assessment (DPIA)	DPIAs are a tool used to identify and minimise the data protection risks of new projects
Criminal Records Information	This refers to personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures and could include DBS checks.